

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

IN RE APPLICATION OF: Takeo HARIU

GAU:

SERIAL NO: NEW APPLICATION

EXAMINER:

FILED: HERewith

FOR: CONCENTRATED SYSTEM FOR CONTROLLING NETWORK INTERCONNECTIONS

REQUEST FOR PRIORITY

ASSISTANT COMMISSIONER FOR PATENTS
WASHINGTON, D.C. 20231

SIR:

- ☐ Full benefit of the filing date of U.S. Application Serial Number, filed, is claimed pursuant to the provisions of 35 U.S.C. §120.
- ☐ Full benefit of the filing date of U.S. Provisional Application Serial Number, filed, is claimed pursuant to the provisions of 35 U.S.C. §119(e).
- ☒ Applicants claim any right to priority from any earlier filed applications to which they may be entitled pursuant to the provisions of 35 U.S.C. §119, as noted below.

In the matter of the above-identified application for patent, notice is hereby given that the applicants claim as priority:

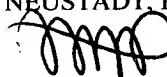
<u>COUNTRY</u>	<u>APPLICATION NUMBER</u>	<u>MONTH/DAY/YEAR</u>
JAPAN	2000-127564	April 27, 2000
JAPAN	2000-178076	June 14, 2000

Certified copies of the corresponding Convention Application(s)

- ☒ are submitted herewith
- ☐ will be submitted prior to payment of the Final Fee
- ☐ were filed in prior application Serial No. filed
- ☐ were submitted to the International Bureau in PCT Application Number .
Receipt of the certified copies by the International Bureau in a timely manner under PCT Rule 17.1(a) has been acknowledged as evidenced by the attached PCT/IB/304.
- ☐ (A) Application Serial No.(s) were filed in prior application Serial No. filed ; and
(B) Application Serial No.(s)
- ☐ are submitted herewith
- ☐ will be submitted prior to payment of the Final Fee

Respectfully Submitted,

OBLON, SPIVAK, McCLELLAND,
MAIER & NEUSTADT, P.C.



Marvin J. Spivak
Registration No. 24,913



22850

Tel. (703) 413-3000
Fax. (703) 413-2220
(OSMMN 10/98)

10978 U.S. PTO
09/842138
04/26/01

日 本 国 特 許 庁

PATENT OFFICE
JAPANESE GOVERNMENT

JCS78 U.S. PTO
09/842138
04/26/01

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日

Date of Application:

2000年 4月27日

出 願 番 号

Application Number:

特願2000-127564

出 願 人

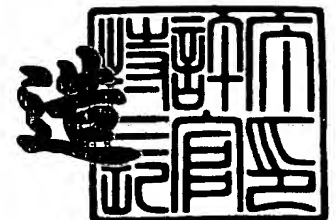
Applicant (s):

日本電信電話株式会社

2001年 4月13日

特許庁長官
Commissioner,
Patent Office

及 川 耕 造



出証番号 出証特2001-3030200

【書類名】 特許願

【整理番号】 NTTH117117

【提出日】 平成12年 4月27日

【あて先】 特許庁長官 殿

【国際特許分類】 H04L 9/32

【発明者】

【住所又は居所】 東京都千代田区大手町2丁目3番1号 日本電信電話株式会社内

【氏名】 針生 剛男

【特許出願人】

【識別番号】 000004226

【氏名又は名称】 日本電信電話株式会社

【代理人】

【識別番号】 100069981

【弁理士】

【氏名又は名称】 吉田 精孝

【電話番号】 03-3508-9866

【手数料の表示】

【予納台帳番号】 008866

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9701413

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 集中型ファイアウォール装置

【特許請求の範囲】

【請求項 1】 複数のユーザ網間接続を行うネットワークに設置されるファイアウォール装置であって、

個々のユーザ網と接続する複数のインタフェースと、

ユーザ網間毎に独立したファイアウォール機能を提供する複数のファイアウォール機能部と、

各インタフェースを複数のファイアウォール機能部のいずれかに対応付ける対応付け機能部とを備えた

ことを特徴とする集中型ファイアウォール装置。

【請求項 2】 対応付け機能部は、各インタフェースとこれらに対応するファイアウォール機能部との関係を管理するテーブルを有し、該テーブルに基づいて各インタフェースを複数のファイアウォール機能部のいずれかに対応付けることを特徴とする請求項 1 記載の集中型ファイアウォール装置。

【請求項 3】 対応付け機能部は、各インタフェースとこれらに対応するファイアウォール機能部との関係を管理するテーブルと、通信を受信したインタフェースに対応するファイアウォール機能部を前記テーブルから検索し、その識別子を通信に付与する識別子付与機能部と、付与された識別子に対応するファイアウォール機能部へ通信を送るファイアウォール識別機能部と、ファイアウォール機能部からの通信に付与された識別子に対応するインタフェースを前記テーブルから検索し、該当インタフェースへ通信を出力する出力インタフェース機能部とからなることを特徴とする請求項 1 記載の集中型ファイアウォール装置。

【請求項 4】 ファイアウォール機能を提供するソフトウェアを複数のプロセスとして同時に動作させることにより、複数のファイアウォール機能部を実現することを特徴とする請求項 1 乃至 3 いずれか記載の集中型ファイアウォール装置。

【請求項 5】 ユーザ網間の接続の許可または拒否を設定するファイアウォールテーブルにファイアウォール機能部を識別する識別子を設けることにより、一

つのファイアウォール機能を複数のファイアウォール機能部として動作させることを特徴とする請求項 1 乃至 3 いずれか記載の集中型ファイアウォール装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、通信のセキュリティ確保のためのファイアウォール装置に関するものである。

【0002】

【従来の技術】

従来より、あるユーザ網に所属するユーザが通信におけるセキュリティを確保しながらその外部または別のユーザ網との間で通信を行う場合、ファイアウォールと呼ばれるセキュリティ機能を用いて通信を行っていた。

【0003】

従来のファイアウォール装置は、装置毎に単一のファイアウォール機能を有するため、異なるユーザ網間毎に個別に装置を設置する必要があった。

【0004】

図 1 は、従来のファイアウォール装置を用いたネットワークシステムの一例を示すもので、図中、1 はネットワーク、1 1, 1 2, 1 3, 1 4 はユーザ網 (USER # 1, USER # 2, USER # 3, USER # 4)、2 1, 2 2, 2 3, 2 4 は各ユーザ網 1 1, 1 2, 1 3, 1 4 に接続されたユーザ端末 (TE # 1, TE # 2, TE # 3, TE # 4)、3 1 はネットワーク 1 に設置された、ユーザ網 1 1 - 1 2 間のファイアウォール装置 (FW # 0 1)、3 2 はネットワーク 1 に設置された、ユーザ網 1 3 - 1 4 間のファイアウォール装置 (FW # 0 2) である。なお、通常、各ユーザ網には複数のユーザ端末が接続されるが、図面では 1 つのみ示した。

【0005】

ユーザ網 1 1 は、ユーザ網 1 2 とファイアウォール装置 3 1 経由で接続され、ファイアウォール装置 3 1 の設定で許可された通信のみ実行可能である。これにより、ユーザ網 1 1 及び 1 2 は各々のセキュリティを確保しつつ、通信を行うこ

とができる。

【0006】

同様に、ユーザ網13は、ユーザ網14とファイアウォール装置32経由で接続され、ファイアウォール装置32の設定で許可された通信のみ実行可能である。これにより、ユーザ網13及び14は各々のセキュリティを確保しつつ、通信を行うことができる。

【0007】

ユーザ網11及び12は、ユーザ網13及び14と全く通信を行わない。従って、セキュリティを確保するため、ユーザ網11及び12と、ユーザ網13及び14とは接続しない。

【0008】

ファイアウォール装置31及び32を単一のファイアウォール装置で実現すると、ファイアウォール装置の内部で、本来、通信のないユーザ間の通信が混じるため、セキュリティを確保することが困難になる。このため、ファイアウォール装置31及び32は別々の装置として実現する必要があった。

【0009】

【発明が解決しようとする課題】

エクストラネットの普及等に伴い、ネットワークを利用するユーザが増加すると、外部との通信または異なるユーザ網間の通信の数も増加する。この場合、個別にファイアウォール装置を設置すると、多数の装置を導入することになり、装置コストが増大するという問題があった。また、別々に設置された多数の装置を管理する必要があり、管理が煩雑になるという問題があった。

【0010】

本発明の目的は、セキュリティを確保した複数のユーザ網間通信を1台の装置で実行可能とすることにより、コストの低減及び管理の省力化を実現できる集中型ファイアウォール装置を提供することにある。

【0011】

【課題を解決するための手段】

本発明では、前記課題を解決するため、複数のユーザ網間接続を行うネットワ

ークに設置されるファイアウォール装置であって、個々のユーザ網と接続する複数のインタフェースと、ユーザ網毎に独立したファイアウォール機能を提供する複数のファイアウォール機能部と、各インタフェースを複数のファイアウォール機能部のいずれかに対応付ける対応付け機能部とを備えたことを特徴とする集中型ファイアウォール装置を提案する。

【 0 0 1 2 】

本発明によれば、各インタフェースに接続されたユーザ網を、対応付け機能部により、予め対応付けられたファイアウォール機能部に接続することができ、これによってユーザ網が多数ある場合においても、ユーザ網毎に個別に装置を必要とせず、1台の装置で複数のユーザ網間通信が実現可能となる。

【 0 0 1 3 】

【発明の実施の形態】

図2は、本発明の集中型ファイアウォール装置を用いたネットワークシステムの一例を示すもので、図中、従来例と同一構成部分は同一符号をもって表す。即ち、1はネットワーク、11, 12, 13, 14はユーザ網（USER # 1, USER # 2, USER # 3, USER # 4）、21, 22, 23, 24は各ユーザ網11, 12, 13, 14に接続されたユーザ端末（TE # 1, TE # 2, TE # 3, TE # 4）、40はネットワーク1に設置された集中型ファイアウォール装置である。

【 0 0 1 4 】

集中型ファイアウォール装置40は、ユーザ網11-12間のファイアウォール機能部（FW # 1）41及びユーザ網13-14間のファイアウォール機能部（FW # 2）を備えている。ファイアウォール機能部41及び42は、インタフェースは異なるが、1台の装置内の機能部として実現される。

【 0 0 1 5 】

ユーザ網11は、ユーザ網12とファイアウォール機能部41経由で接続され、ファイアウォール機能部41の設定で許可された通信のみ実行可能である。これにより、ユーザ網11及び12は各々のセキュリティを確保しつつ、通信を行うことができる。

【 0 0 1 6 】

同様に、ユーザ網 1 3 は、ユーザ網 1 4 とファイアウォール機能部 4 2 経由で接続され、ファイアウォール機能部 4 2 の設定で許可された通信のみ実行可能である。これにより、ユーザ網 1 3 及び 1 4 は各々のセキュリティを確保しつつ、通信を行うことができる。

【 0 0 1 7 】

ユーザ網 1 1 及び 1 2 は、ユーザ網 1 3 及び 1 4 と全く通信を行わない。従って、セキュリティを確保するため、ユーザ網 1 1 及び 1 2 と、ユーザ網 1 3 及び 1 4 とは接続しない。

【 0 0 1 8 】

図 3 は、本発明の集中型ファイアウォール装置の実施の形態の一例を示すもので、図中、A、B、C、D はそれぞれユーザ網 1 1、ユーザ網 1 2、ユーザ網 1 3、ユーザ網 1 4 が接続されるインタフェース、4 1、4 2 はファイアウォール機能部、4 3 は各インタフェース A ～ D をファイアウォール機能部 4 1、4 2 に対応付ける I / F - F W 対応付け機能部である。

【 0 0 1 9 】

複数のインタフェース A ～ D は、複数のユーザ網を接続するために使用する。

【 0 0 2 0 】

複数のファイアウォール機能部 4 1、4 2 は、ユーザ網間毎に独立したファイアウォール機能を提供するために使用する。複数のファイアウォール機能部 4 1、4 2 は、同一装置内においてファイアウォール機能を提供するソフトウェアを複数のプロセスとして同時に動作させることにより、実現可能である。また、ユーザ網間の接続の許可または拒否を設定するファイアウォールテーブルにおいて、検索キーにファイアウォール機能部を識別する識別子及び方向を追加することにより、一つの前記プロセスを複数のファイアウォール機能部として動作させることも可能である。

【 0 0 2 1 】

図 4 は、I / F - F W 対応付け機能部の詳細を示すもので、予め設定した、入力及び出力インタフェースとこれらに対応するファイアウォール機能部との関係

を管理するファイアウォール機能管理テーブル431と、通信を受信したインタフェースに対応するファイアウォール機能部をテーブル431から検索し、その識別子を通信に付与する識別子付与機能部432と、付与された識別子に対応するファイアウォール機能部へ通信を送るファイアウォール識別機能部433と、ファイアウォール機能部からの通信に付与された識別子に対応するインタフェースをテーブル431から検索し、該当インタフェースへ通信を出力する出力インタフェース識別機能部434とからなっている。

【0022】

図5は、I/F-FW対応付け機能部の動作例を示すものである。

【0023】

ユーザ網から通信を受信すると、識別子付与機能部432がファイアウォール機能管理テーブル431を検索し、通信を受信した入力インタフェース、例えばAに対応するファイアウォール機能識別子及び方向、ここではFW#1及びI/F#1→I/F#2を取得し、これを通信に付与して、ファイアウォール識別機能部433に送信する。

【0024】

ファイアウォール識別機能部433は、通信に付与された前記ファイアウォール機能識別子及び方向に基づき、通信に対応するファイアウォール機能部41（FW#1）に送信する。

【0025】

出力インタフェース識別機能部434は、ファイアウォール機能部41（FW#1）で処理された通信を受け取ると、ファイアウォール機能管理テーブル431を検索し、該通信に付与されたファイアウォール機能識別子及び方向に対応する出力インタフェース、ここではBを取得し、この出力インタフェースBに送信する。

【0026】

図6は、ファイアウォール機能管理テーブルの一例を示すものである。本テーブルは集中型ファイアウォール装置に設定され、入力及び出力インタフェースとこれらに対応するファイアウォール機能部との関係を管理する。このテーブルに

より、集中型ファイアウォール装置は、インタフェースによってユーザ網を識別し、異なるユーザ網間の通信を別々に処理することが可能となる。また、異なるユーザが重複したネットワークアドレスを使用している場合に、通信を受信したインタフェースにより、ユーザを識別することが可能になる。

【0027】

図7は、ファイアウォールテーブルの一例を示すもので、本テーブルは集中型ファイアウォール装置に設定され、ファイアウォール機能管理テーブルで設定されたファイアウォール機能部毎にファイアウォールを設定する。このテーブルにより、各ユーザ網間の接続の許可または拒否の設定が可能になる。

【0028】

テーブルの項目にファイアウォール機能識別子及び方向を追加することにより、一つのプロセスを複数のファイアウォール機能部として動作させることができる。ファイアウォールテーブルにファイアウォール機能識別子及び方向の項目を設け、通信に付与されたファイアウォール機能識別子及び方向を検索キーとして検索することにより、通信に対するファイアウォール動作を決定することができる。異なるユーザ網からの通信は、ネットワークアドレスが同一であっても、入カインタフェースの違いにより異なるファイアウォール機能識別子が付与されるため、独立なファイアウォールとして動作できる。

【0029】

【発明の効果】

以上説明したように、本発明によれば、ユーザ網が多数ある場合においても、ユーザ網毎に個別に装置を必要とせず、1台の装置により複数のユーザ網間接続を実現でき、低コストで容易に管理可能なユーザ網間接続を実現できる。

【図面の簡単な説明】

【図1】

従来のファイアウォール装置を用いたネットワークシステムの一例を示す構成図

【図2】

本発明の集中型ファイアウォール装置を用いたネットワークシステムの一例を

示す構成図

【図 3】

本発明の集中型ファイアウォール装置の実施の形態の一例を示す構成図

【図 4】

I / F - F W 対応付け機能部の詳細を示す構成図

【図 5】

I / F - F W 対応付け機能部の動作例を示す図

【図 6】

ファイアウォール機能管理テーブルの一例を示す図

【図 7】

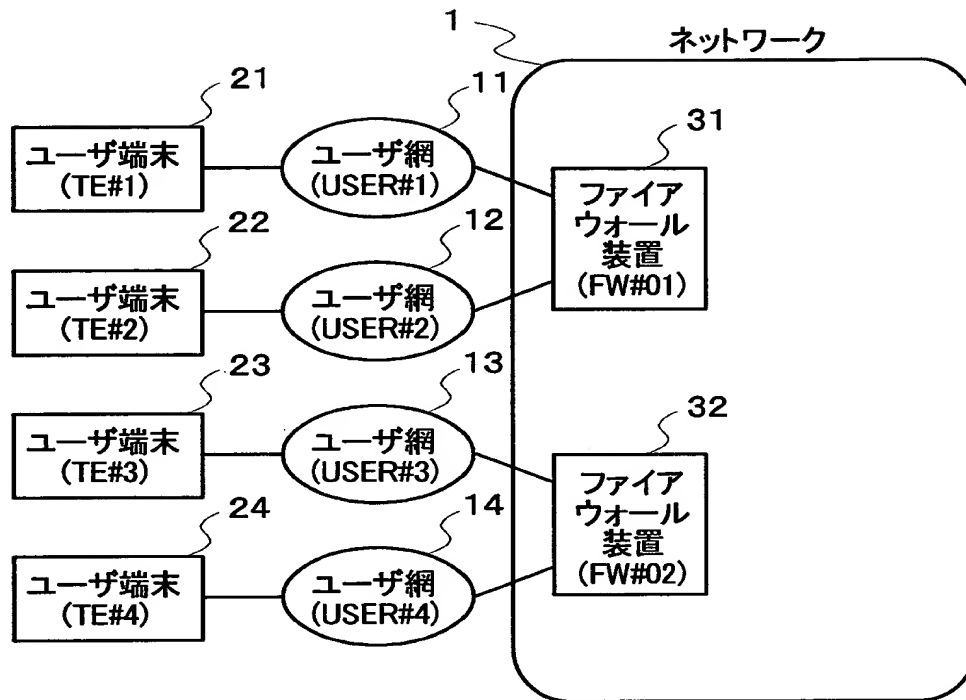
ファイアウォールテーブルの一例を示す図

【符号の説明】

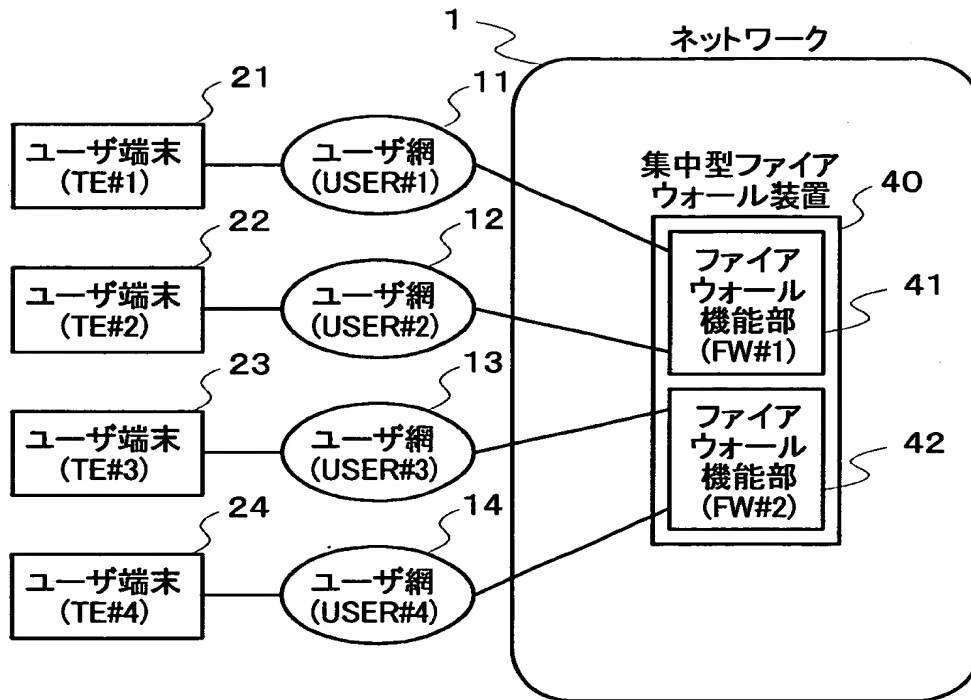
1 : ネットワーク、11 ~ 14 : ユーザ網 (USER # 1 ~ USER # 4)、
21 ~ 24 : ユーザ端末 (TE # 1 ~ TE # 4)、40 : 集中型ファイアウォール装置、41, 42 : ファイアウォール機能部 (FW # 1, FW # 2)、43 :
I / F - F W 対応付け機能部、431 : ファイアウォール機能管理テーブル、4
32 : 識別子付与機能部、433 : ファイアウォール識別機能部、434 : 出力
インタフェース識別機能部、A ~ D : インタフェース。

【書類名】 図面

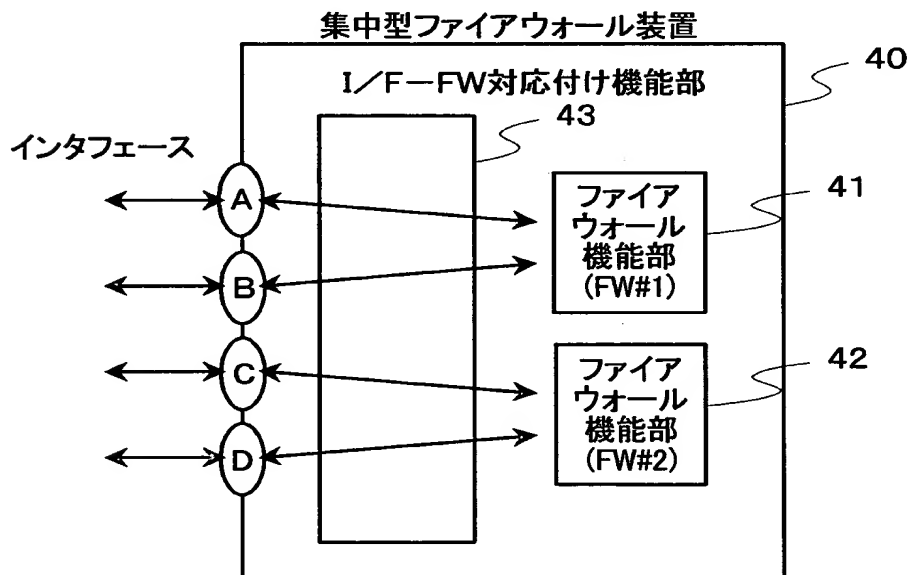
【図 1】



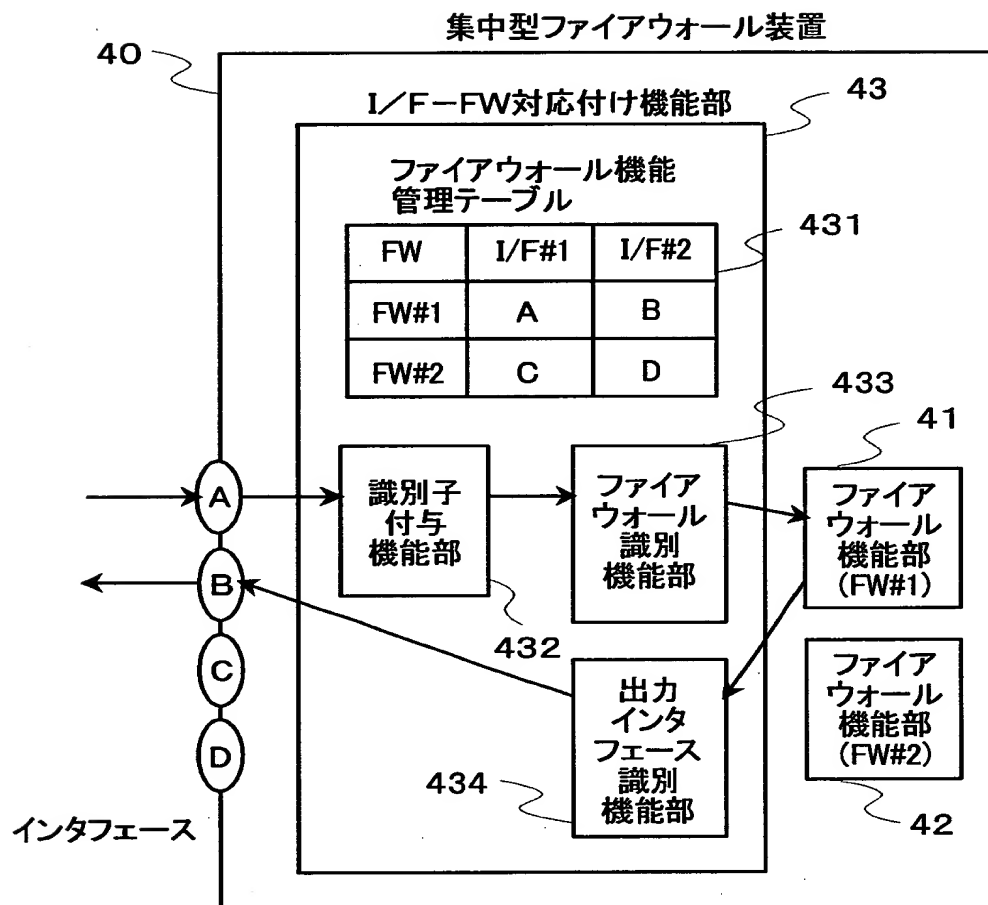
【図 2】



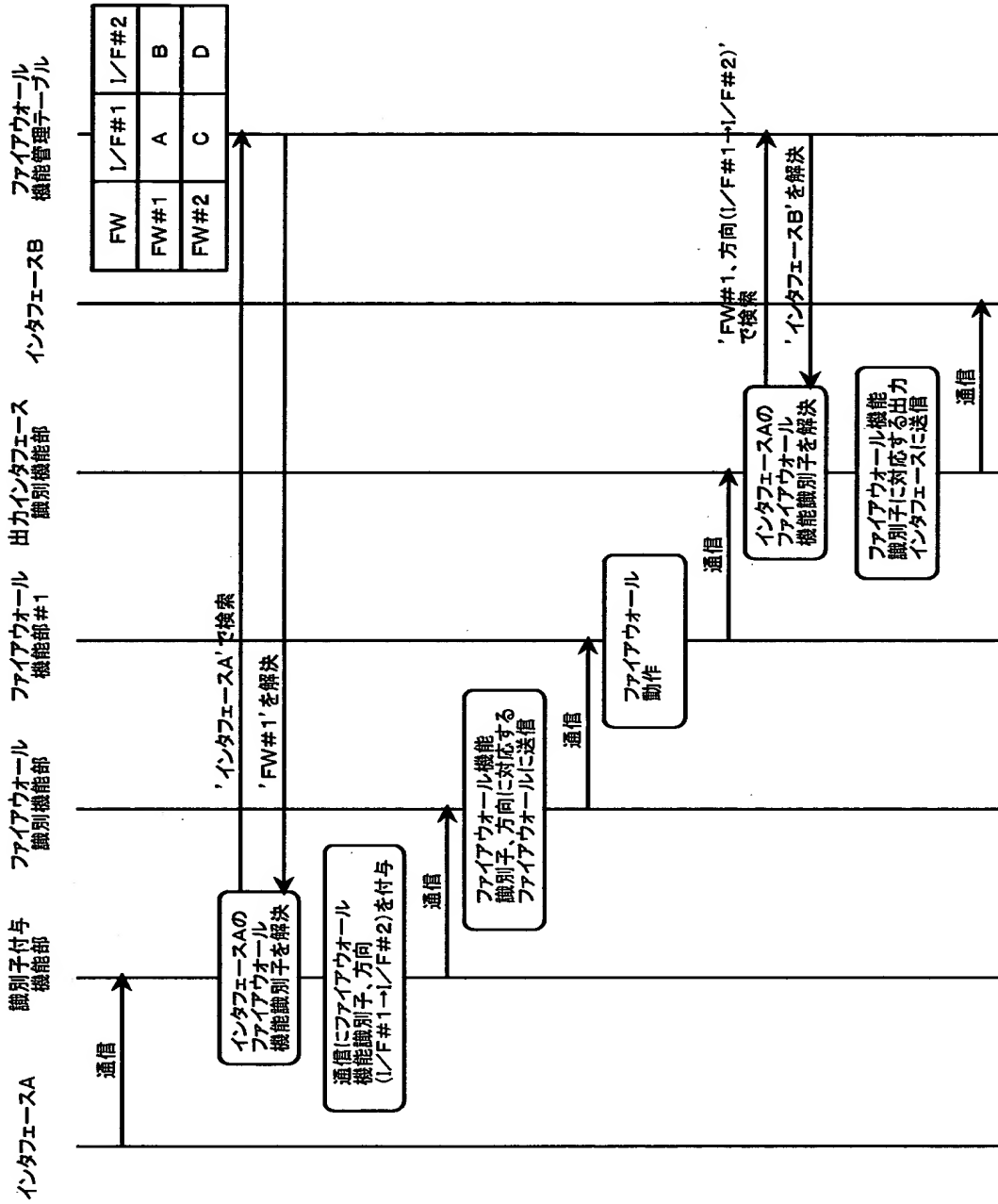
【図 3】



【図 4】



【図 5】



【図 6】

ファイアウォール 機能識別子	インタフェース1	インタフェース2
FW#1	A(USER#1)	B(USER#2)
FW#2	C(USER#3)	D(USER#4)
⋮		⋮

【図 7】

FW機能 識別子	方向	発端末 アドレス	着端末 アドレス	アプリケーション 種別	動作
FW#1	I/F1→2	a	c	AA	許可
FW#1	I/F1→2	b	d	BB	拒否
FW#1	I/F2→1	c	a	BB	許可
FW#1	I/F2→1	d	b	AA	許可
FW#2	I/F1→2	a	c	BB	拒否
FW#2	I/F1→2	b	d	BB	許可
FW#2	I/F2→1	c	a	AA	許可
⋮	⋮	⋮	⋮	⋮	⋮

【書類名】 要約書

【要約】

【課題】 セキュリティを確保した複数のユーザ網間通信を1台の装置で実行可能とすることにより、コストの低減及び管理の省力化を実現すること。

【解決手段】 個々のユーザ網と接続するインタフェースA～Dと、ユーザ網間毎に独立したファイアウォール機能を提供するファイアウォール機能部41, 42と、各インタフェースA～Dをファイアウォール機能部41, 42に対応付ける対応付け機能部43とを備えたことにより、各インタフェースA～Dに接続されたユーザ網を、予め対応付けられたファイアウォール機能部41, 42に接続し、セキュリティを確保した複数のユーザ網間通信を1台の装置で実行可能とする。

【選択図】 図3

出 願 人 履 歴 情 報

識別番号 [0 0 0 0 0 4 2 2 6]

1. 変更年月日	1 9 9 9 年 7 月 1 5 日
[変更理由]	住所変更
住 所	東京都千代田区大手町二丁目 3 番 1 号
氏 名	日本電信電話株式会社